



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/786,824	06/07/2001	Walter Strohbeck	10191/1739	6516

26646 7590 06/15/2004

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER

ZIMMERMAN, BRIAN A

ART UNIT

PAPER NUMBER

2635

9

DATE MAILED: 06/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/786,824

Applicant(s)

STROHBECK, WALTER

Examiner

Brian A Zimmerman

Art Unit

2635

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 March 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 30-59 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 30-59 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

EXAMINER'S RESPONSE

Status of Application

In response to the applicant's amendment received on 3/24/04. The examiner has considered the new presentation of claims and applicant arguments in view of the disclosure and the present state of the prior art. And it is the examiner's position that claims 30-59 remain unpatentable for the reasons set forth in this office action:

This case has been reassigned to a different examiner. Accordingly, all correspondence regarding this case should reflect the new examiner.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

1. Claims 30-38, 40-45, 47-52, and 54-58 are rejected under 35 U.S.C. 102(b) as being anticipated by Hirozawa et al. (heretofore Hirozawa, EP 0695675 A1).

In reference to claim 30, Hirozawa provides a method for key verification for use with a security system (Abstract), the security system including at least one valid key (1) and an electronic verification arrangement having a transceiver for communicating with the key (2,3), the electronic verification arrangement (2, 3, 7, 8) storing unique identification data for the key and storing enable data

Art-Unit: 2635

corresponding to the unique identification data for the key (5, 6, 10, 11 store the enabling identification data), the electronic verification arrangement generating an authority for accessing a secured object (4, 9) when authentication data is received from the key (1), the method comprising the steps of;

- Accessing the unique identification data for the key in a mode of the security system (Col 14, lines 5-11).
- Performing a predetermined procedure to enter a key validation mode of the security system the step of performing the predetermined procedure being performed by a user of the security system (Col 14, lines 12-16).
- Retaining enable data for each of the keys within a transceiver range in the key validation mode (Col 14, lines 16-18, transceiver range is defined by the area very close to the ignition).
- Deleting other enable data for each of the keys outside the transceiver range in the key validation mode (Col 14, lines 16-18).
- Deactivating each of the keys for which the other enable data is deleted in the step of deleting (Col 14, lines 16-18).

In reference to claim 31, claim 30 is taught as above. Hirozawa teaches that the predetermined procedure includes a vehicle starting procedure (Col 14, lines 12-16).

In reference to claim 32, claim 30 is taught as above. Hirozawa teaches that the predetermined procedure includes a vehicle access procedure (Col 14,

Art. Unit: 2635

lines 11-14). The deactivation of the immobilizer unit is seen a vehicle access procedure. In addition, vehicle-starting procedure is also seen as a vehicle access procedure.

In reference to claim 33, claim 30 is taught as above. Hirozawa teaches that the predetermined procedure includes a standard vehicle procedure using a standard vehicle control. Claim 33 is taught as claim 31 above. The ignition switch is seen as a standard vehicle control, which would be used in a standard vehicle procedure.

In reference to claim 34, claim 33 is taught as above. Hirozawa teaches that the standard vehicle control includes an ignition switch. Claim 34 is taught as claim 31 above.

In reference to claim 35, claim 33 is taught as above. Hirozawa teaches that the predetermined procedure includes a vehicle starting procedure, the steps of the starting procedure are performed at different times than times for performing the standard vehicle procedure (Col 14, lines 11-16, car ignition is turned on off not to drive but to initiate key verification sequence).

In reference to claim 36, claim 30 is taught as above. Hirozawa teaches that indication of completion of key validation code is performed by not placing another key in the keyhole in a predetermined amount of time of about 4 seconds (Col 14, lines 18-21).

In reference to claim 37, claim 30 is taught as above. Hirozawa teaches that a display is generated for an activated valid key of the security system to

Art-Unit: 2635

indicate completion of validation by turning on interior lights through the use of an indicator (16). (Col 8, lines 21-26).

In reference to claim 38, claim 30 is taught as above. Hirozawa teaches that the keys used for disarming the security system do not have activating buttons. It is clear that Hirozawa, when speaking of keys, is talking of a lock-opening device such as a key for a tumbler lock (although not a said specific limitation) with a transponder attached to the device (Col 2, lines 27-31).

In reference to claim 40, claim 30 is taught as above. Hirozawa teaches that the authority (immobilizer (4), EGI (9)) allows access to the secured object (vehicle).

In reference to claim 41, claim 40 is taught as above. Hirozawa teaches that the secured object is a vehicle (Abstract).

In reference to claim 42, claim 30 is taught as above. Hirozawa teaches that the secured object is a vehicle and the authority allows operation of the vehicle (immobilizer (4), EGI (9) control operation of the vehicle).

In reference to claim 43, claim 42 is taught as above. Hirozawa teaches that included in operation of the vehicle is starting the vehicle (Col 2, lines 26-31).

In reference to claim 44, Hirozawa teaches of a security system that comprises

- At least one valid key (1)
- An electronic verification arrangement including a transceiver for communicating with at least one valid key and including a mode for accessing unique identification data (transponder (1))

Art-Unit: 2635

communicates with immobilizer and EGI unit (4, 9) through antenna (2) to access unique identification data) wherein the electronic verification arrangement is operable to

- Store the unique identification data for at least one valid key (memory 5, 6, 10, 11)
- Generate an authority for accessing a secured object when authentication data is received from a valid key (ignition power, IG1 is controlled through immobilizer and EGI unit)
- Store enable data in accordance with the unique identification data for each activated one of the valid keys (memory 5, 6, 10, 11)
- Enter a key validation mode when a user performs a predetermined procedure (Col 2, lines 27-31)
- Retain enable data for each of the valid keys within a transceiver range in the key validation mode (Col 14, lines 16-18, transceiver range is defined by the area very close to the ignition)
- Delete other enable data for each of the valid keys outside the transceiver range in the key validation mode (Col 14, lines 16-18)

In reference to claim 45, claim 44 is taught as above. Claim 45 is taught as claim 31 above.

Art Unit: 2635

In reference to claim 47, claim 44 is taught as above. Claim 47 is taught as claim 33 above.

In reference to claim 48, claim 47 is taught as above. Claim 48 is taught as claim 34 above.

In reference to claim 49, claim 47 is taught as above. Claim 49 is taught as claim 35 above.

In reference to claim 50, claim 44 is taught as above. Claim 50 is taught as claim 36 above.

In reference to claim 51, claim 44 is taught as above. Claim 51 is taught as claim 37 above.

In reference to claim 52, claim 44 is taught as above. Claim 52 is taught as claim 38 above.

In reference to claim 54, claim 44 is taught as above. Claim 54 is taught as claim 40 above.

In reference to claim 55, claim 54 is taught as above. Claim 55 is taught as claim 41 above.

In reference to claim 56, claim 44 is taught as above. Claim 56 is taught as claim 42 above.

In reference to claim 57, claim 56 is taught as above. Claim 57 is taught as claim 43 above.

In reference to claim 58, Hirozawa teaches of an anti-vehicle-thief apparatus (Title) thus intended use is for a vehicle. Additional limitations of claim 58 taught as in claim 44 above.

Art Unit: 2635

Thus, Hirozawa teaches all the limitations of claims 30-38, 40-45, 47-52, and 54-58.

2. Claim 44 and 46 is rejected under 35 U.S.C. 102(b) as being anticipated by Castleman.

In reference to claim 44, Castleman teaches of a security system comprising

- At least one valid key (20)
- An electronic verification arrangement including a transceiver (21) for communicating with at least one valid key (20) and including a mode for accessing unique identification data (Mode activated upon insertion of the key into transceiver 21) herein the electronic verification arrangement is operable to
 - o Store the unique identification data for at least one valid key (12)
 - o Generate an authority for accessing a secured object when authentication data is received from a valid key (14,16)
 - o Store enable data in accordance with the unique identification data for each activated one of the valid keys (EEPROM 32)
 - o Enter a key validation mode when a user performs a predetermined procedure (Insertion of a master key into lock, Col 10, lines 1-15)

Art Unit: 2635

- Retain enable data for each of the valid keys within a transceiver range in the key validation mode (enable data is retained for valid keys, Col 10, lines 1-15)
- Delete other enable data for each of the valid keys outside the transceiver range in the key validation mode (Deletion of all keys, Col 10, lines 64-67).

In reference to Claim 46, claim 44 is taught as above. Castleman describes a procedure for entering the key validation sequence, which comprises placing a master key into the locking mechanism, of which the procedure is also used for unlocking a door (Fig 1 shows door setting, Col 10, lines 1-15 describe validation sequence). Castleman also teaches that his invention be used in different settings including that of a vehicle (Abstract).

Claim Rejections - 35 USC § 103

3. Claims 39 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirozawa.

In reference to claim 39, claim 30 is taught as above. Hirozawa remains silent as to security code access procedure including the storing of enable data for the unique identification data. It would have been obvious to one skilled in the art at the time of invention to transmit enable data (control information) between the key and the verification unit in order to protect the secrecy of the unique identification number stored on the key. Transmission of enable data (control

Art Unit: 2635

code) that has been encrypted by a numeric algorithm using the identification number as a seed when both sender and receiver know the seed is a typical in the industry and considered a "safe" access procedure as the identification number is not sent and thus cannot be replicated. Such rolling code sequences are considered enabling data since only the key and transmitter know the next such "enabling" code number. Choosing enable data to consist of only one byte (8 bits) rather than a smaller or larger number of bits would have been within the design choice of the security of the encrypting code.

In reference to claim 53, claim 44 is taught as above. Claim 53 is taught as claim 39 above.

Thus, it would have been obvious to one skilled in the art at the time of invention to combine the teachings of Hirozawa with that of known prior art to transmit a control byte or bytes as necessary to implement a secure rolling code algorithm.

Response to Arguments

Applicant's arguments filed 3/24/04 have been fully considered but they are not persuasive.

The applicant argues that Hirozawa does not disclose retaining enable data for each valid key within a transceiver range in the validating mode, and deleting enable data for keys not within the transceiver range. As the applicant points out, Hirozawa provides a manner in which the ID code from a valid key is

Art Unit: 2635

registered (thereby retaining enable data) by inter alia, placing the key in the ignition of the vehicle. To require placing of the key in the ignition is within the scope of the broadly claimed "inside the transceiver range." In other words when the key is in the ignition it is inside the transceiver range. The applicant also admits on page 13 of the response 3/24/04, that all other keys are then deleted. This reads on deleting data for keys not within the transceiver range. Again the applicant, discussing Hirozawa, states that additional keys can then be programmed by placing the key(s) in the ignition which is within the scope of the broadly claimed "within the transceiver range."

The applicant argues that Castleman does not teach retaining enable data for each valid key within a transceiver range in the validating mode, and deleting enable data for keys not within the transceiver range. As the applicant points out, Castleman provides a manner in which the ID code from a valid key is registered (thereby retaining enable data) by inter alia, touching the lock with the key in a certain manner. To require touching the lock with the key is within the scope of the broadly claimed "inside the transceiver range." In other words when the key is touching the lock it is inside the transceiver range. The applicant also admits on page 16 of the response 3/24/04, that all other keys are then deauthorized. This reads on deleting data for keys not within the transceiver range.

Art Unit: 2635

The applicant attempts to destroy the examiner's rejection of claims 39 and 53 by requesting an affidavit and questioning the motivation of the combination. Nowhere, however, has the applicant pointed to a limitation that exists in the claim yet is not shown by the references. Claim 39 (and claim 53) requires that the enable data include a control byte. The ID information transmitted from the key to the immobilizer unit and stored in both the immobilizer unit and the EGI unit can be considered control information as broadly claimed by the applicant. Since the limitation is taught by the reference, as broadly claimed, an affidavit is not required.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian A Zimmerman whose telephone

Art Unit: 2635

number is 703-305-4796. The examiner can normally be reached on Off every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mike Horabik can be reached on 703-305-4704. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Brian A Zimmerman
Primary Examiner
Art Unit 2635

BAZ